Linguistic Encryption for Underwater Communication

OLIVIA BLANCHETTE*, GABRIELLE CALDERON†‡, ANDREW HAMBY*, JING LIU*, VALERIIA RUBANOVA†, AND VINCENT MOONEY*†

†SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING, *SCHOOL OF COMPUTER SCIENCE, ‡SCHOOL OF MODERN LANGUAGES

GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA, USA

presented at MECO'2024 and CPSIoT'2024, Budva, Montenegro, June 11-14

www.mecoconference.me

Authors from Undergraduate Research

- Georgia Tech has an undergraduate research program called Vertically Integrated Projects (VIP) leading to satisfy accreditation design requirements
- This team is 5 undergraduates plus A/P Mooney

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Introduction

We propose an encryption scheme for underwater gliders which employs a simple yet robust constructed language to represent commands.

A stream cipher provides security features and dolphin sounds are used as acoustic signals.

Background – Underwater Gliders

- Underwater unmanned autonomous vehicles (UUAVs) have become increasingly prevalent in research and commercial applications
  - Typically use acoustic networks for communication
  - Low power usage allows for long-term missions without human intervention

- The underwater environment and low-power requirements make security difficult
  - UUAVs are vulnerable to eavesdropping, spoofing, and more
  - Standard secure protocols cannot be used underwater

Background – Language

- Toki Pona is a constructed language with a limited number of phonemes
  - Possible to implement any command with 140 morphemes
  - Table I shows the complete list of Toki Pona phonemes

TABLE I
TOKI PONA ALPHABET

Consonants	j, k, l, m, n, p, s, t, w
Vowels	a, e, i, o, u

- Aquatic mammals, namely dolphins and whales, communicate underwater using clicks and whistles
  - A variety of sounds are used to convey complicated information

Background – RanCode

- RanCode is a pseudorandom permutation generator which uses an ephemeral key to produce encodings

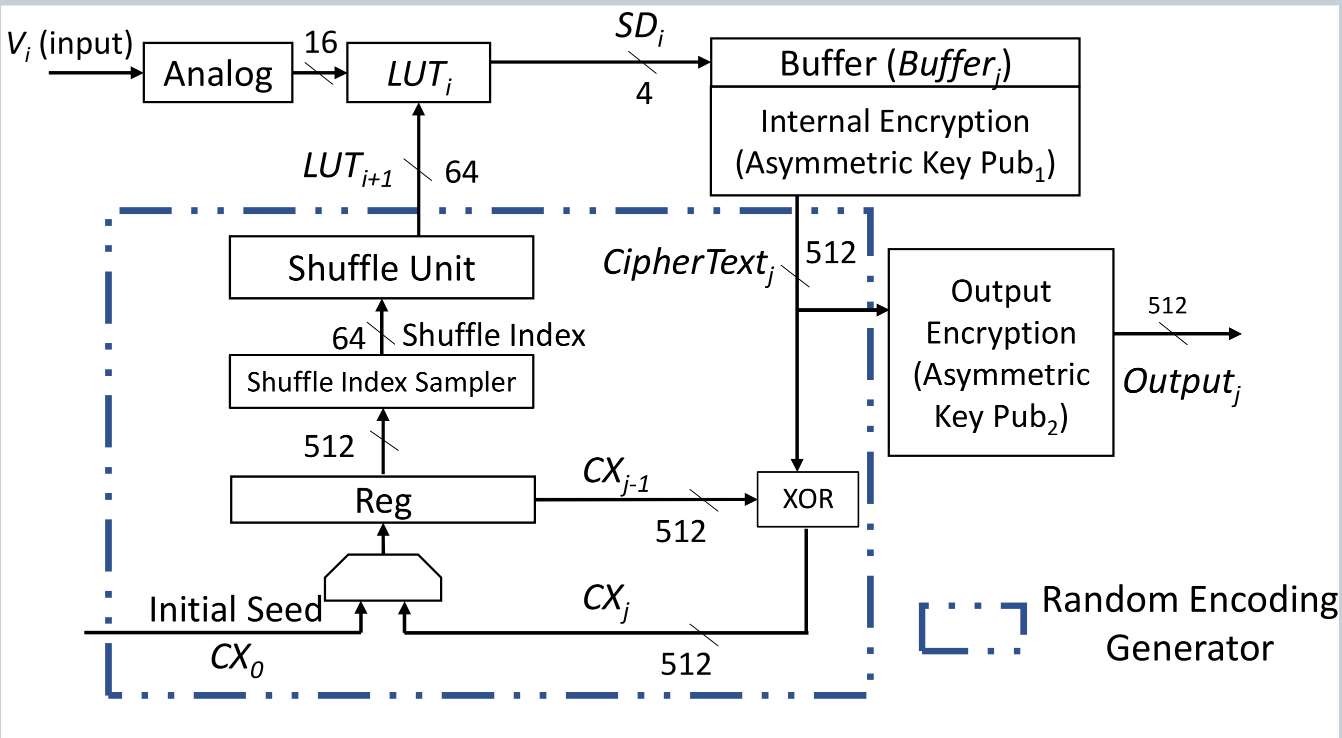


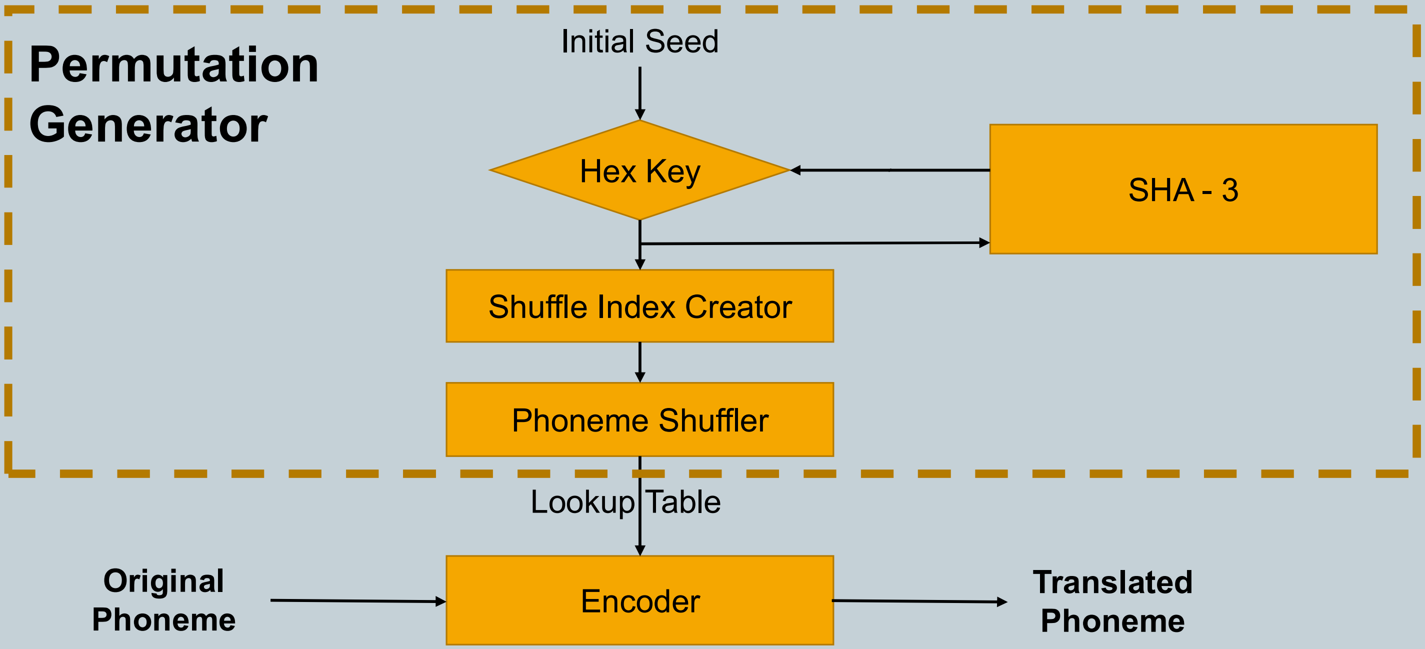
Figure 5: Full Diagram of Rancode Architecture

A complete overview of Rancode architecture

Hutto, Kevin, and Vincent J. Mooney. "Sensing with random encoding for enhanced security in embedded systems." 2021 10th Mediterranean Conference on Embedded Computing (MECO), IEEE, 2021.

Background – RanCode

- Encodings are deterministic
  - Two devices with the same seed and inputs will have the same output after the same number of iterations
- Permutations are created using a Knuth shuffle in combination with a self-updating SHA-3 hash



Permutation Example

Original: en

Hex Key: 0A47...

LUT1: e -> a

New Hex Key: 8357...

LUT2: n -> d

Encoded: ad

Original	LUT1	LUT2
a	k	n
e	**a**	e
i	x	j
o	j	t
u	o	p
k	l	i
l	n	x
m	t	u
n	e	**d**
p	i	l
s	s	a
t	x	m
w	m	o
j	d	k
d	u	w
x	w	s

Permutation Example

Original: en

Hex Key: 0A47...

LUT1: e -> a

New Hex Key: 8357...

LUT2: n -> d

Encoded: ad

Original	LUT1	LUT2
a	k	n
e	**a**	e
i	x	j
o	j	t
u	o	p
k	l	i
l	n	x
m	t	u
n	e	**d**
p	i	l
s	s	a
t	x	m
w	m	o
j	d	k
d	u	w
x	w	s

Permutation Example

Original: en

Hex Key: 0A47...

LUT1: e -> a

New Hex Key: 8357...

LUT2: n -> d

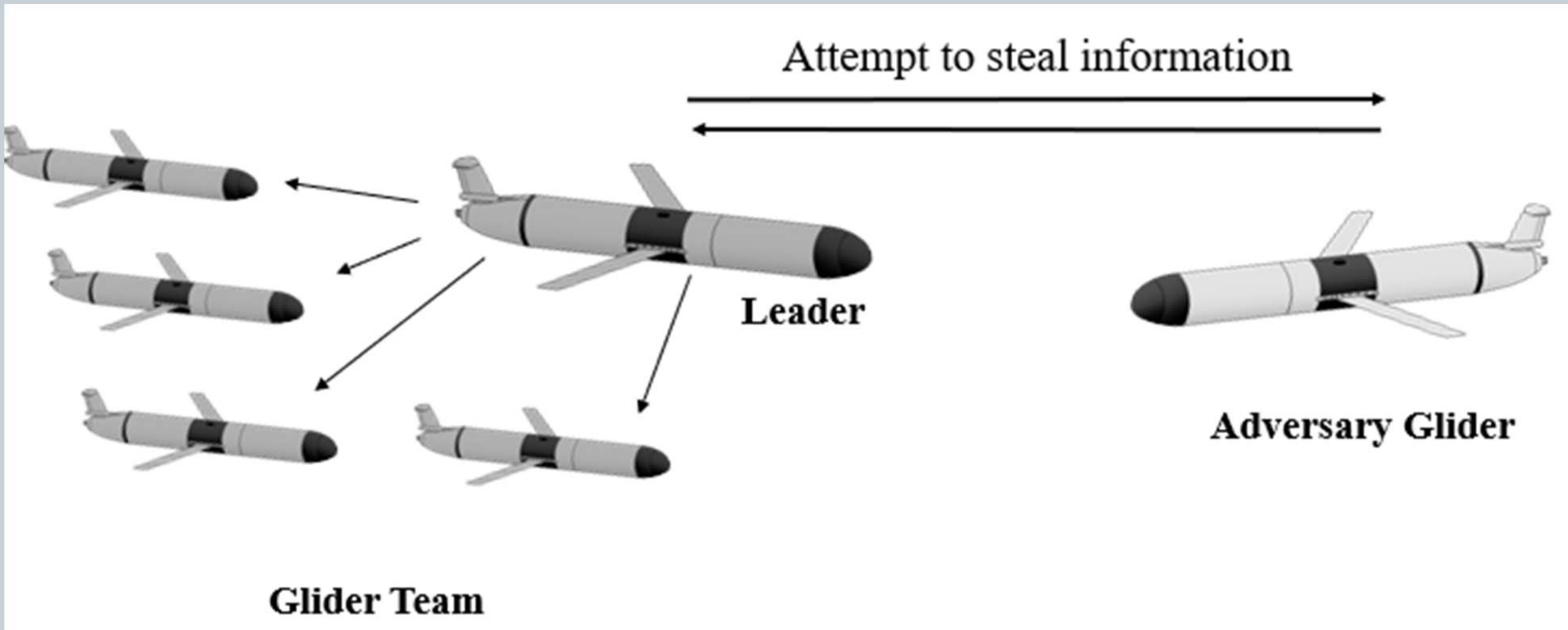
Encoded: ad

Original	LUT1	LUT2
a	k	n
e	**a**	e
i	x	j
o	j	t
u	o	p
k	l	i
l	n	x
m	t	u
n	e	**d**
p	i	l
s	s	a
t	x	m
w	m	o
j	d	k
d	u	w
x	w	s

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Scenario



This figure shows the proposed use case scenario for our communication scheme: a leader glider sending commands to follower gliders, with an adversary attempting to intercept the acoustic signals

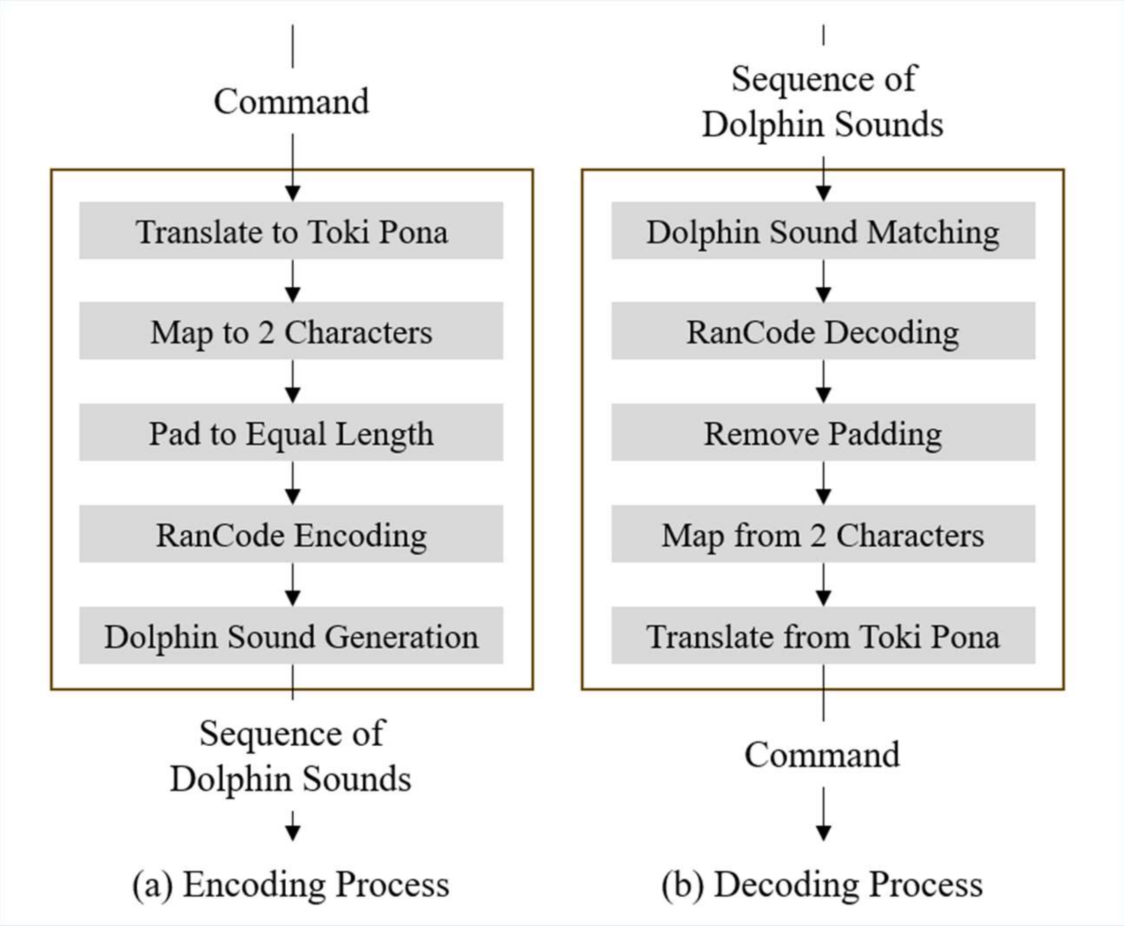
Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Linguistic Methodology

This diagram provides an overview of the entire encoding process performed by the leader from command to acoustic signal.

The process is done in reverse by each follower to decode commands.



Linguistic Methodology

Table II shows how commands are represented in Toki Pona, mapped to simple encodings, and padded to a standard length.

TABLE II
SCENARIO COMMANDS, TOKI PONA, TWO-CHARACTER MAPPING

Command	Toki Pona	Mapping	Padding
North	sewi	aa	aa dd
Northeast	suno sewi	ae aa	ae aa
East	suno open	ae ai	ae ai
Southeast	suno anpa	ae ao	ae ao
South	anpa	ao	ao dd
Southwest	anpa suno	ae au	ae au
West	suno pini	au	au dd
Northwest	sewi suno	am	am dd
Stop	pini	au	au dd
Watch	lukin	am	am dd
Forward **	sinpin **	ak **	ak **
Backward **	monsi **	al **	al **

Table III shows how numbers can be represented

TABLE III
DIGIT MAPPINGS

Digit	0	1	2	3	4	5	6	7	8	9
Toki Pona Mapping	a	e	i	j	k	l	m	n	o	p

Linguistic Methodology

Table II shows how commands are represented in Toki Pona, mapped to simple encodings, and padded to a standard length.

Table III shows how numbers can be represented

TABLE II
SCENARIO COMMANDS, TOKI PONA, TWO-CHARACTER MAPPING

Command	Toki Pona	Mapping	Padding
North	sewi	aa	aa dd
Northeast	suno sewi	ae aa	ae aa
East	suno open	ae ai	ae ai
Southeast	suno anpa	ae ao	ae ao
South	anpa	ao	ao dd
Southwest	anpa suno	ae au	ae au
West	suno pini	au	au dd
Northwest	sewi suno	am	am dd
Stop	pini	au	au dd
Watch	lukin	am	am dd
Forward **	sinpin **	ak **	ak **
Backward **	monsi **	al **	al **

TABLE III
DIGIT MAPPINGS

Digit	0	1	2	3	4	5	6	7	8	9
Toki Pona Mapping	a	e	i	j	k	l	m	n	o	p

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Encryption Methodology

- Commands are encoded character by character using look up table permutations generated by RanCode
- The pseudorandom permutations are unpredictable for an adversary without the seed (key)
- The same seed (key) is initially synchronized across gliders to allow for secure decoding

Outline

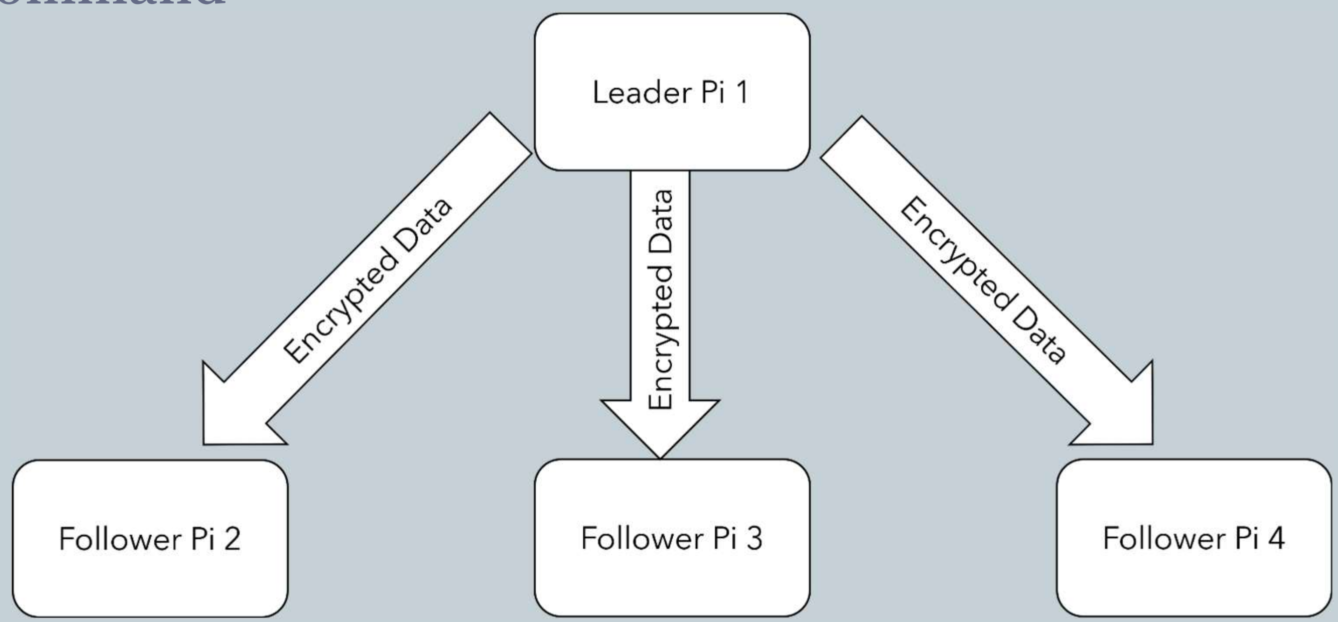
- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Experimental Setup

The system architecture was configured to mimic our identified use case scenario using Raspberry Pis

Experimental Setup

- Raspberry Pis are assigned Leader and Follower roles and communicate via chatroom
  - Commands are entered into the Leader Pi, encoded, and transmitted
  - Each Follower Pi independently receives, decodes, and displays the command



Experimental Results

- Commands were properly decoded by the Follower Pis, as shown in Table IV
- Each representation has no interpretable relation to the initial command or previous encodings

TABLE IV
COMMAND COMMUNICATION

Leader Cmd	Broadcast	Pi 2 Display	Pi 3 Display	Pi 4 Display
South	mpas	South	South	South
Forward 45	axom	Forward 45	Forward 45	Forward 45
Northwest	tjjd	Northwest	Northwest	Northwest
South	eidu	South	South	South
Stop	ssaw	Stop	Stop	Stop
Watch	sddu	Watch	Watch	Watch

Experimental Results

- Commands were properly decoded by the Follower Pis, as shown in Table IV
- Each representation has no interpretable relation to the initial command or previous encodings

TABLE IV
COMMAND COMMUNICATION

Leader Cmd	Broadcast	Pi 2 Display	Pi 3 Display	Pi 4 Display
South	mpas	South	South	South
Forward 45	axom	Forward 45	Forward 45	Forward 45
Northwest	tjjd	Northwest	Northwest	Northwest
South	eidu	South	South	South
Stop	ssaw	Stop	Stop	Stop
Watch	sddu	Watch	Watch	Watch

Experimental Results

- Commands were properly decoded by the Follower Pis, as shown in Table IV
- Each representation has no interpretable relation to the initial command or previous encodings

TABLE IV
COMMAND COMMUNICATION

Leader Cmd	Broadcast	Pi 2 Display	Pi 3 Display	Pi 4 Display
South	mpas	South	South	South
Forward 45	axom	Forward 45	Forward 45	Forward 45
Northwest	tijd	Northwest	Northwest	Northwest
South	eidu	South	South	South
Stop	ssaw	Stop	Stop	Stop
Watch	sddu	Watch	Watch	Watch

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Practical Extensions

- Integration with GPS coordinates could improve glider control
  - Can extend movement commands into three dimensions
  - Movement optimization possible
- Quaternion-based movement provides several advantages
  - Eliminate singularities and edge cases
  - Allows for more robust and reliable control

Outline

- Intro & Background
- Scenario
- Linguistic Methodology
- Encryption Methodology
- Experimental Setup & Results
- Practical Extensions
- Conclusions

Conclusions

- We have demonstrated a proof-of-concept for an encryption scheme which leverages Toki Pona and Rancode for lightweight, secure communication
- We verified our design using an implementation on Raspberry Pis
  - Future work will confirm the design in an underwater environment
- Later extensions might integrate GPS coordinates or quaternion-based commands for greater control

THANK YOU

Q&A